BOISE STATE UNIVERSITY

Boise State University

SECURITY CAMERA & ALARM ASSESSMENT

JANUARY 2014

MARGOLIS HEALY®
SOLUTIONS FOR SAFE CAMPUSES®

Boise State University
SECURITY CAMERA & ALARM ASSESSMENT
JANUARY 2014 Report

MARGOLIS HEALY®
SOLUTIONS FOR SAFE CAMPUSES®

TABLE OF CONTENTS

STATEMENT OF NEED

Boise State is Idaho's metropolitan research university, located in the state's population center and capital city. Boise is an ideal place to live – a hub of government, business, the arts, recreation, health care, industry and technology. In its 81st year, Boise State is truly coming of age in higher education. Award-winning faculty, students, alumni and staff have put Boise State on the map with breakthrough research and records of achievement.

Boise State is the largest university in Idaho with 22,678 students. The university offers studies in nearly 200 fields of interest. Undergraduate, graduate, doctoral and technical programs are available in seven colleges: Arts and Sciences, Business and Economics, Education, Engineering, Graduate Studies, Health Sciences, and Social Sciences and Public Affairs. Through partnership opportunities and relationships close to home, Boise State is dedicated to research, innovation and student experiences that drive economic development and contribute to a vibrant and healthy community.

With more than 200 student organizations, a location near downtown Boise and area recreation, and university residence halls along the scenic Boise River Greenbelt, the campus provides opportunities for both education and adventure. Students can study abroad or within the community, participate in one of the largest internship programs in the Northwest, and work with professors on progressive research.

Under the leadership of Jon Uda, Executive Director of Campus Security and Police Services, the University retained our services to conduct an independent review of the school's current use of security cameras and alarm systems compared with contemporary standards and to make recommendations that will enhance the school's security posture. Our assessment identifies gaps in the program and makes recommendations to close those gaps in the most efficient and cost effective manner possible.

ORGANIZATION OF THIS REPORT

This report is presented in a chapter format with five major sections. Section I describes the Methodology for the assessment, Section II includes Essential Challenges, Section III outlines our General Observations, Section IV our Specific Observations and Recommendations, and finally, Section V is our Master List of Recommendations. The recommendations in this section address the areas in which we believe the school has the opportunity to make improvements to meet current best, promising or acceptable practices. In addition, multiple attachments addressing specific policies and/or graphic illustrations are included at the end of the report.

ACKNOWLEDGMENTS

Margolis Healy & Associates acknowledges the assistance and guidance of Jon Uda, Executive Director of Campus Security and Police Services; Jill Fedigan, Capital Educational Facilities Planner; and Christy Jordan, Director of Capital Planning; who served as our primary liaisons for this project. We extend our appreciation to members of the Boise State faculty, staff and students who were instrumental in providing the appropriate context and historical information about the school, Campus Security operations, and the evolution of the school's use of security cameras, alarms and other security related systems. Without exception, everyone was welcoming, forthcoming and honest in his or her opinions and thoughts. Boise State was truly a gracious host.

DISCLAIMER AND DISCLOSURE

Margolis Healy & Associates conducted this assessment and prepared this report at the request of Boise State University. The authors' opinions, findings, conclusions, and recommendations are provided solely for the use and benefit of the school. Any warranties (expressed and/or implied) are specifically disclaimed. Any statements, allegations, and recommendations in this report should not be construed as a governing policy or decision unless so designated by other documentation. The report is based on the most accurate data gathered and available to Margolis Healy & Associates at the time of the assessment and presentation. Our recommendations are subject to change in light of changes in such data.

SECTION I – METHODOLOGY

MHA conducted an objective assessment of Boise State University's use of security cameras and alarm systems and its policies and procedures in accordance with the school's wishes. Additionally, we emphasized the use of security cameras for outdoor or "exterior" locations around the campus. The primary focus of this assessment was to evaluate the overall effectiveness of the school's use of these technologies compared with contemporary standards or best and promising practices in higher education and identify gaps and/`or challenges in the use and management of these systems.

MHA accomplished this by conducting a review of the current staffing of the Boise State Campus Security Department (relative to its security systems), as well as any policies and procedures against acceptable, promising and reasonable practices in education safety and security. MHA conducted substantive research, document reviews, site visits, and interviews to become familiar with Boise State University and its use of electronic security systems.

This included numerous unescorted and random tours of the campus during the day and evening that were not announced to the community and were aimed at identifying areas of risk and concern. Much of our focus was particularly focused on areas connecting the main campus to off-campus locations and on areas where student are known to walk at night.

The team, consisting of MHA Senior Director Daniel Pascale and Associates Paul Allena and Michael Kwiatkowski, visited the Boise State campus on two separate occasions for a total of six days. The team first visited the University during July and again in late October of 2013. During the site visits, the team reviewed the areas under consideration, conducted interviews in one-on-one and group sessions, and met with members of the Department's leadership.

Our approach to this assessment included an in-depth examination of the following core areas:

- The use of security cameras
- The use of alarm systems
- Written directives, policies & procedures (system related)
- Systems integration
- Operational staffing (related to security systems)

MHA reviewed a compendium of documents that included but was not limited to the following:

- Boise State access control policy
- Boise State Campus Security standard operating procedures
- Boise State Campus Security organizational charts

- Boise State buildings list
- Boise State Annual Security Report
- Boise State Fire Alarm Systems Report
- Boise State key control policy
- Site Assistance Visit (SAV) Report

The information contained herein serves three general audiences and purposes. First, the research and findings are organized to provide the University's leadership with a concise set of actionable items. Second, leadership can use the detailed information found in the observations to understand specific areas of structure, policy and practice they should address. Third, the executive summary provides the University community with an understanding of the orientation to the assessment.

SECTION II – ESSENTIAL CHALLENGES

1. Use of Security Technology – Physical Security Approach

The University deploys several different forms of security technology as part of its overall physical security program. The use and growth of these systems, however, seems to have developed organically rather than as part of the University's strategic plan or vision. In fact, we believe the University lacks a clear strategy, defined leadership and/or ownership of security systems.

Several University departments play a role in the administration of these systems but no one department owns them. For example, the policy states that Facilities is responsible for electronic access control, the Campus Security Department houses and monitors security cameras, intrusion and fire alarms; and IT provides back-end and technical support as well as alarm programming and training.

During our interviews with University stakeholders, which included staff and students, we consistently heard that no one actually knows who is responsible for security systems and technology and no one knows to whom they would go to if needed to add technology or had a recurring problem. We were not surprised by this based on our initial findings and the decentralized environment of security systems at Boise State.

2. Program Management

Managing modern security systems such as complex security cameras, digital and network video recording, intrusion and duress alarm systems and software has become a full-time job at many institutions.

It is important to understand the difference between the technical management of security systems and the strategic, organizational management related to systems installation and integration.

We do not believe that Boise State currently has someone serving in this capacity with the necessary knowledge, skills and abilities to move the program forward from both a technical and strategic perspective. As previously mentioned, the decentralized approach to security systems and technology has led to disparate systems throughout the campus, as well as a lack of integration and accompanying policy.

3. Design Standards

Based on our observations and discussions, we concluded that there is no single vision for the use of security cameras or alarm systems at Boise State. We did not see a consistent standard throughout the campus for the deployment of cameras or intrusion detection systems. Nor did we see design standards for new facilities or those being retrofitted. In fact, there was an ongoing discussion while we were on campus regarding the deployment of

multiple panic alarms within a facility because the facility had requested them. However, the University cannot respond to such requests appropriately because it does not have a standard or a risk-based decision matrix that dictates the appropriate use of these alarms.

Furthermore, we learned during our interviews that key players in the decision-making process are not always included in project meetings at an early stage. Those responsible for the deployment of various security systems are not always included in the planning phase of projects, which can lead to inconsistent levels of security as well as additional post construction work and expenses such as retrofitting to pull wire, add Internet cable drops, etc.

4. Policies and Procedure

It was apparent to us that Boise State significantly lacks an institutional policy regarding the use of security cameras and intrusion detection systems.

We asked Boise State to provide MHA with copies of any and all policies, procedures and related documents relevant not only to security systems and technology in general but also specifically to security cameras and alarm systems. We also requested these documents when speaking with staff during our visits to campus.

We were not provided with, nor were we able to locate, any University policies related to standards on the acceptable use, purchase or design of security cameras or intrusion detection systems. We did receive a copy of a 2008 policy related to general access control and access control systems that assigned responsibility for these systems to Facilities and Housing. A lack of policies can potentially lead to waste, misuse, needless duplication of effort or equipment, and general confusion over “who does what.”

SECTION III – GENERAL OBSERVATIONS

Based on our interactions with Boise State University administrators, staff and students and other members of the Boise State community, we are confident that the University is committed to fostering a safe and secure campus environment, while simultaneously ensuring that it is appropriately open and inviting. The University has taken, and continues to take, significant steps to enhance campus safety, specifically by deploying security cameras, intrusion and duress alarms, emergency phones, electronic access control and other security- related countermeasures.

However, we are concerned that there may be a perception of security that does not live up to the reality due to the organic growth of these systems and the decentralized nature of their placement. One example of this decentralization is that the University did not have an accurate accounting of all the security cameras and alarms that are deployed on campus at the time of our visit. In other words, the individuals in charge of the systems were not positive where cameras were placed, what type of cameras were used, how video was stored, etc. This appears to be the byproduct of individual departments contacting various vendors on their own over several years, even decades, and installing their own individual systems.

We heard different perceptions of the school's use of cameras during interview with students. For example, some people feel cameras placed around the campus provided a sense or feeling of "safety and security," while some students believe that the cameras are continuously monitored by an operator who could send help them in an emergency. Others were surprised to learn that the University does not have more cameras, particularly in areas such as the Greenbelt and the stadium parking lot.

"Security is both a reality and a feeling," according to security expert Bruce Schneier. "The reality of security is mathematical, based on the probability of different risks and the effectiveness of different countermeasures."1 We know the probability of having an active shooter on a given campus is extremely low. We also know the cost of addressing the threat of an active shooter, and can thus calculate whether or not committing funds to such tactics (i.e., more police, guns, security, etc.) is cost effective. But Schneier states that security is also a feeling, based on individual psychological reactions to both the risks and the countermeasures. And the reality and the feeling about security are two different things: You can be secure even though you don't feel secure, and you can feel secure even though you're not secure in reality. There are times when people feel less secure than they actually are. In those cases, a palliative countermeasure that primarily increases the feeling of security may be just what the doctor ordered. This can take the form of emergency blue light phones, an overt security camera or countless "panic" or duress buttons found at many universities and colleges.

Schneier (2008) goes on to argue that like real security, "*Security Theater*" has a cost. It can cost money, time, concentration, personal freedom and so on. It can also come at the cost of reducing the other things we can do. Security theater is usually a bad trade-off because the costs far outweigh the benefits. But there are instances when a little bit of *Security Theater* makes sense. We can make smart security trade-offs when our feeling of security closely matches the reality. When the two are out of alignment, we are much more likely to get security wrong. *Security Theater* is no substitute for security reality, but used correctly it can be a way of raising our feeling of security so that it more closely matches the reality of security by bringing us closer to how we would feel if we had all the facts and did all the math correctly."

Boise State is no different than other institutions that, at times, struggle with finding the appropriate mix and use of security systems and technology such as cameras, emergency phones and alarms. Whether weighing such measures against the campus culture, community concerns over privacy or diminishing budgets, every institution strives to find the appropriate balance of countermeasures to match perception with reality.

The Department of Campus Security and Police Services (later referred to as Campus Security), led by Jon Uda is responsible for the overall safety and security of students, faculty, staff and visitors at Boise State University. However, we found that the department is not wholly responsible for, in control of or financially able to design, install, select and manage the various security systems in use on campus.

We believe this is one factor that has led to the lack of strategic vision for the further use of security cameras and alarms and the integration of these systems to work more efficiently in a centralized, security operations center. It appears that no single entity has been able to significantly advance the use of these systems because the university has not appropriately designated an "operational owner" for them.

As mentioned in our essential challenges, the University faces two additional challenges that we believe can be largely mitigated once the University has formally determined an "operational owner" for security systems and technology. These challenges are the lack of policy and procedures and design standards.

We believe that the decentralized approach to these systems has resulted in no one taking the responsibility to address these needs. For example, the management of electronic access control systems has been formally delegated to the Facilities Department. The Facilities Department has therefore appropriately developed a policy regarding the use and management of electronic access control systems.

The University should strive to develop consistent standards for the use of electronic security systems throughout the campus and through its many facilities. For example, the deployment of cameras, alarms and other

technologies should largely be the same or similar for residential facilities, as well as for administrative buildings, academic buildings, etc. However, there may be exceptions of facilities that have a heightened risk, such as chemical laboratories, which would require a different security presence based on the contents of the space. This is a common practice throughout college and universities.

Equipment standards are equally important. We feel the University must determine the appropriate manufacturers, models and software platforms to efficiently and appropriately integrate the current disparate systems with future systems. This endeavor that should not be assigned to a single entity but should instead be part of an interdepartmental committee representing a wide cross section of stakeholders at the University.

Finally, we feel the University should continue to expand its use of security cameras, particularly in less populated areas where community members are known to walk or congregate at night. Based on our interviews, we believe Campus Security is keenly aware of these areas and continually seeks opportunities to provide a physical presence while determining the appropriate use of supportive technologies.

All that we have witnessed and learned leads us to believe that, with adjustments and support in the areas we have identified, Boise State University will have a model physical security program that provides a reasonable level of security, while continuing to offer a welcoming and vibrant campus environment.

SECTION IV – SPECIFIC OBSERVATIONS

USE OF SECURITY TECHNOOGY - PHYSICAL SECURITY APPROACH

Contemporary Standard

Colleges and universities have increasingly embraced the use of electronic security systems and security technology to enhance campus safety. When properly integrated into a comprehensive physical security program, these systems can serve as an effective force multiplier, supplementing police, security personnel and others deployed in the security role.[1] Many components comprise a physical security program, including geography, positive barriers, signage and lighting, electronic security systems and technology such as security cameras. However, electronic access control and intrusion detection systems play a critical role in the overall security program. This role continues to evolve as technology advances and is readily available on the public market.

At a minimum, an effective security system, including security technology, should include the following:

a. Design standards;

b. Appropriate policies;

c. Standardized equipment and the efficient integration of this equipment; and,

d. Program management.

An institution should strive to maintain consistent security practices throughout its campus or be able to articulate why a particular security measure has been implemented in one place but not another. It is also important to implement security technology systems that can be integrated with legacy systems and expanded later as technology evolves and the institution's overall physical security program changes. The decision to implement electronic security systems is one that requires significant research, planning and coordination based on an institution's specific circumstances, including its culture, resources, precipitating events, and security management capacity.

The adoption of campus-wide security standards represents one promising practice that many institutions have embraced as they adopt security technology as a fundamental part of their comprehensive physical security program. The overall goal of these standards is to ensure that the institution is "security-smart" and is committing resources in a wise and efficient manner. The standards should include building-specific security system designations and standardized security platforms and systems for specific types of buildings and areas of campus. For example, many institutions have designated three basic security levels:

[1] ASIS International, "Systems Integration, Part I," in *Protection of Assets Manual* (ASIS International, Alexandria, Va., 2004).

a. Protection Level I – Academic/administrative buildings: card access systems, intrusion alarms in designated areas;

b. Protection Level II – Residence halls, medium security areas: card access, intrusion alarms, security cameras;

c. Protection Level III – Laboratories, critical areas, and office spaces for key college administrators; all of the above, advanced access control, additional levels of intrusion detection systems, and other systems as needed.

Equally important to the implementation and management of these systems is the need for comprehensive policies and procedures regarding the acceptable use of security systems, training requirements, maintenance and authority. Policies are necessary not only to guide the implementation of systems and provide the framework for procedures but they also should describe how the systems will be used, by whom and under what circumstances.

At a minimum, the institution should adopt a single policy that incorporates a framework for the overarching physical security program. Institutions are increasingly beginning to develop policies that govern the use of each system, i.e., specific policies for security cameras, access control, alarm systems, emergency phones, etc.

In an ideal situation, the responsibility for managing the security systems and technology program should be centralized and aligned in the appropriate department. Since the culture of institutions can differ greatly, the decision regarding where the responsibility for program management will report is one that should be made on a case-by-case basis. It is almost standard for institutions to dedicate a full-time FTE position to manage and direct the security technology program.

Collaboration among the various departments and functional areas on campus is a critical to the overall success of the physical security program. The individual responsible for security systems and technology should become the chief steward who ensures appropriate collaboration between the Campus Security Department, Facilities, Information Services, Housing/Residential Life, and other constituent groups, as needed.

Observations

Our primary objectives for this assessment were to evaluate Boise State's use of security cameras and alarm systems against reasonable, best and promising practices in higher education security and leverage these technologies to enhance overall campus safety and security.

To meet this objective, the team needed to understand how the University approaches the use, deployment and management of security systems and technology and how, if at all, that approach integrates with the overarching physical security program. We will discuss our observations based on

contemporary standards as to how Boise State can enhance its posture in these areas, and we will identify areas that we believe require additional attention.

To this end, we examined the interrelationships of three major areas: people, policy and equipment/technology. Our goal was to understand the current physical system(s) deployed on campus (i.e., security cameras, alarms, and electronic access control); supporting policies/procedures, and the people responsible for the selection, deployment, and management of these systems.

It became clear during our interviews with those who have a stake or role in security system deployment that the University lacks a strategic vision and ownership of these systems. We were not provided with, nor were we able to locate, any University policies related to the acceptable use, purchase or design standards for security cameras or alarms. While not entirely in the scope of this assessment, we have also considered the use of electronic access control because of its close interrelationship with other technical security countermeasures. We were provided with a policy for the use of electronic access control that was written and published by the Facilities Department.

We independently interviewed and discussed the use and management of current security systems and technology deployed throughout the campus with members of the Boise State Campus Security Staff, IT, Housing, students, and others. Nearly every person we interviewed had the same response related to the responsibility for these systems. They stated that while they have some role in the security systems, and are willing to assist each other and work together, they do not have primary stewardship for the overall management of security systems. Additionally, no one believes he or she currently has the resources to effectively manage the University-wide systems.

While this decentralized arrangement may be intentional in this case, this type of arrangement often leads to inefficient practices, inconsistent procedures and a lack of coordinated services. For example, dispatchers or clerks in the Campus Security Department often view security cameras although they do not view them continuously. However, Campus Security does not have a complete or accurate list of all the cameras on campus, access to those cameras or the ability to set equipment or design standards for them.

Based on what we learned in our interviews, Campus Security is often looked to for guidance in regards to cameras and alarms, yet they have had little or no say in how and why these systems have been deployed. Instead, those decisions have typically been made at the local department level with or without an established process. This system has taken the place of a university standard such as a needs assessment or risk analysis to determine the appropriate use of security systems and ensure that the placement of any device falls within reasonable and accepted practice and University policy. In our professional opinion, it is critical for the University to adopt standards that are equally applied during the decision-making process.

Another example involves policies related to security systems and technology in general and security cameras and alarm systems specifically. As mentioned earlier in this section, the University was unable to provide MHA with any policies related to design standards, not only for buildings and facilities but all University property.

This lack of a documented, systematic approach can lead to inconsistent standards and security practices throughout the campus and may also inhibit the University's ability to leverage vendor relationships. This mix and match application also sends confusing messages to community members who question why security systems or other countermeasures are used in one building or area of the campus but not another.

It is important to note that we have a great deal of confidence in the competency of each department to carry out the assignments and roles they are currently assigned related to security systems and technology. For example, it is clear that IT has the technical management skills to support these systems from a design and integration standpoint. Likewise, it is clear that the Facilities staff are well versed in the use of electronic access control, and that Campus Security leadership has a clear vision for the strategic implementation of security systems. However, we again emphasize that the lack of a formal operational or "business owner" does not lend itself well to creating synergies among the various stakeholders and implementing security systems in a comprehensive manner that enhances campus safety and security.

We believe, based on our observations, information gathering and experience, that the Boise State Campus Security Department should be the sole operational or "business owner" of security systems and security technology on the Boise State University campus. Campus Security is responsible from an operational standard for all aspects of campus security. It also has personnel available 24x7 and the department is most likely to require either recorded video, access logs or alarm reports during or after a specific incident. In addition, the Boise Police are housed with Campus Security and their personnel are available to utilize these systems during critical incidents or routine evaluation.

We are confident based on all that we know and all that we have learned that this can be accomplished with the proper allocation of resources, including human capital. The Department of Campus Security is not only positioned to carry this effort forward and advance Boise State's security posture, but they are, in fact, eager to do so. This would include the integration of technical systems, the installation of exterior security cameras and the integration of various alarm systems into one, 24 x 7 centralized security operations center on campus.

That said, the University will need to commit the necessary resources to ensure effective management and appropriate collaboration between Campus Security, Facilities, Information Technology, Housing & other stakeholders regardless what department the University designates as the business owner.

Based on our findings, this will likely be accomplished through the creation of a new position such as manager or director of Security Systems and Technology, reporting directly to the Executive Director of Campus Security and Police Services. This position should become the primary source for all security systems and technology deployment at the University. The individual assigned to this position should not only be technically competent in electronic security systems, camera deployment, recording devices and standards, but also well versed in conducting site security surveys and risk-based facility assessments to determine the appropriate use of security systems and other countermeasures.

It is also reasonable that this position would directly supervise the security operations center, which includes overseeing the monitoring of these systems by Boise Police Dispatchers. This would be advantageous as there is currently no formal training in the use of these systems from the University to the staff.

It may or may not be necessary to add additional staff to support this new position in order to build a sound program. For example, there may, in fact, be someone already at the University who has the necessary knowledge, skills and abilities to assume this position. If so, there are benefits to promoting from within the organization. Candidates inside the University are likely to have the institutional knowledge transfer and cultural competency and require minimal additional training as well as reducing the cost of selection.

We also observed that the University has a number of disparate security systems in place. In our experience, this is not uncommon but clearly does not support the University's ability to integrate and centralize all of its systems. Having design standards and policy can greatly reduce the opportunity for disparate systems to emerge and also increase the likelihood that systems can be centralized through integration.

The University has made a significant investment in the various systems we expect to see on college and university campuses, including emergency phones, access control, security cameras, alarm systems and a mass notification system. We will discuss the use of cameras and alarms in further detail in subsequent sections of the report.

Understanding that the speed and evolution of technology is often changing faster than systems can be installed, we believe it is imperative that a formalized group of key stakeholders meet on a regular basis to ensure policies and standards are followed, and that they are consistently reviewed for relevance and changes in technology. This would essentially be a working group dedicated to security technology.

This multi-constituent group should include representatives from the appropriate departments and divisions that have functional and strategic responsibility for safety and security, along with undergraduate, graduate and commuter students. The group's primary objectives would be to develop security technology standards and policies; review and approve security technology

measures; ensure collaboration and inclusion of security technology standards during major renovations; and serve as strategic planners.

Recommendations

1. Create a new position responsible for security systems and technology including but not be limited to the development of security technology standards, design standards, oversight of security systems, systems integration and physical security surveys and assessments. This individual would report to the Security Technology Working Group.
2. Establish campus-wide security standards. Campus-wide security standards are a promising practice that institutions are implementing as they commit considerable resources to security technology. The overall goal of such standards is to ensure that buildings are "security-smart" given reasonably foreseeable threats and available resources. These standards should include building-specific security technology system designations that specify the types of security systems that the University would expect for specific types of buildings.
3. Assign the Department of Campus Security as the formal operational or "business owner" of security technology and security systems.
4. Create a Security Technology Working Group. The individual holding the new position referenced in recommendation #1 should chair this committee.
5. Develop campus-wide security technology system equipment standards. Determine common equipment hardware, manufacturers, models, capacities and software that are easily integrated with other systems at the University.
6. Select a nationally recognized value added reseller (VAR) with the capacity to meet the needs of the University to purchase and install University-approved security systems while leveraging centralization to reduce overall costs.
7. Develop comprehensive policies related to each specific security technology. These policies should not only cover the purpose, scope and acceptable use of each technology but also the procurement process.
8. Engage in a campus-wide assessment to identify and inventory all security systems currently being utilized throughout the University. These should at least include security cameras, intrusion alarms, duress alarms, and electronic access control readers.
9. Wherever possible, make an effort to integrate disparate legacy security systems to one common platform that includes all devices and security system countermeasures that terminate at the Campus Security building. Under the current system, individual departments that have previously installed security systems replace or upgrade these systems

on an as needed basis. However, we can only assume that that service, maintenance, and upgrades are completed because the University is not aware of all the systems currently in place. Integrating systems will ensure that all systems are integrated and maximize the University's return on investment.

10. As the University embarks on the development of University-wide security standards and facility design standards, we suggest an initiative to ensure that all existing building security systems comply with the new standards. Clearly, this is a process that must be phased in over a period of years based on available time and resources.

SECURITY CAMERAS

Contemporary Standard

A properly integrated security camera system can provide an effective force multiplier, supplementing security personnel and others deployed in the security role. The system can allow the University to use its security officers to provide a highly visible presence and to interact with community members in positive ways.

Security cameras can be used in one of two basic ways: surveillance mode and alarm assessment mode. The surveillance mode allows the communications officer/operator to conduct routine and directed video patrols of specified locations. This use significantly enhances the security presence by providing additional eyes and even ears on the campus. In the alarm assessment mode, the system triggers real-time sounding of alarms that indicate unauthorized or otherwise unwanted activity. When operated and managed as intended, an alarm assessment system enhances the campus security officers' ability to rapidly respond to acts that impact campus safety and security.

The deployment of any security tool should be based on evidence that points to its effectiveness in enhancing campus safety and/or increasing community members' sense of security. This is obviously true of security cameras as well. Unfortunately, there have been no substantive surveys or research conducted with respect to the effectiveness of security camera effectiveness on college or university campuses. Anecdotally, campus administrators will state that cameras have a positive impact on their respective campuses. Based on personal conversations with campus public safety executives at institutions where cameras have been heavily deployed and articles published in newspapers, we surmise that the camera deployments at those locations have had a significant impact on crime and have increased the campus's sense of security.

In a research survey conducted in the United Kingdom in 2005 entitled "Assessing the Impact of CCTV," the authors found mixed results in their control study. According to the paper, "Out of the 13 systems evaluated, six showed a relatively substantial reduction in crime in the target area compared

[2]Martin Gill and Angela Spriggs, Home Office Research Study 292, *Assessing the impact of CCTV*, (February 2005).

with the control area, but only two showed a statistically significant reduction relative to the control, and in one of these cases the change could be explained by the presence of confounding variables." The paper further points out that camera deployment had more positive results in certain types of areas such as parking facilities and residential areas.[2] We met with multiple security personnel in order to understand the University's Security Department operations, including Department management. We also spoke with faculty, staff and students who are familiar with the Department.

Observations

Boise State University currently utilizes between 80 to 100 cameras, many of which are connected to the Lenel-OnGuard video management platform. As we have pointed out during the course of this report, this number is an approximation since the University is aware that disparate systems exist but cannot accurately account for all of them.

These cameras report back to the Campus Security Department and while several cameras are displayed on monitors near the dispatcher workstation, they are not monitored on a routine basis as a matter of policy. Like many colleges and universities, the primary benefit of security cameras is to deter criminal behavior and aid administrators and/or authorities during a post incident investigation.

From what we were told and observed, the University utilizes multiple camera types including fixed cameras, pan tilt, zoom or "PTZ" cameras in both analog and digital configurations throughout the campus. There does not appear to be a clear standard in place at this time. Not only does the University lack a standard that spells out when and where security cameras will be used, there also is no clear equipment standard in place. While Margolis Healy does not endorse one manufacturer, model or type of camera over another, we support the selection of standard cameras such as fixed, PTZ, day/night, color, mega pixel, digital, etc.

We believe that much of this problem is directly related to the lack of ownership in camera systems. Because the installation of cameras was largely unregulated for many years, (meaning departments largely did their own thing), standards were not adopted or adhered to. This is true, for example, at locations such as the Taco Bell Arena, where the operators of the Arena have installed their own security camera system that is not integrated with the Campus Security Department and does not follow a recognized standard or conform to a camera policy.

It should be noted that the Campus Security Department has made great strides over the past few years in reaching across departmental lines in an attempt to standardize camera types and influence cameras placement. We believe this is a positive aspect of the overall camera program at Boise State and reflects well on the current management team and supporting administration.

We heard complaints from multiple groups regarding the quality of video. In fact, more than one individual with knowledge of the security cameras advised us that video quality is of such poor quality that the videos provide little or no probative value in cases in which reviewing video of incidents under investigation would usually be most valuable.

While we did not review the individual screen images of each camera at the University, we did observe several cameras that presented blurry or pixelated images, had dark shadows or were simply too far or not properly aligned to capture the desired image to aid Campus Security staff. We recognize that these circumstances may be temporary in some cases due to direct sunlight or a temporary system failure but it is important to note these observations since they seem to support a general perception of the system by its users that it works poorly.

We cannot stress enough the value of standardizing equipment and platforms of open architecture that can be integrated with each other. Integrated systems allow for more efficient use of technology leading to a greater return on investment and allowing the technology to work.

For example, it would be valuable to integrate the video management and access control systems. A common alarm with an electronic access control system is a "propped/held open" and/or "forced open" alarm that sounds when one of these conditions is present. If a camera is present at the door, the operator will often go into a separate system to attempt to retrieve video to investigate the cause of the alarm. This is often a manual process that can take several minutes and delay the investigation. By integrating video with the access control systems and alarms, an operator will be alerted as soon as \an alarm is triggered and any video coverage of the area will automatically appear at the operator's station. This eliminates the need for a manual search and decreases the time needed to conduct an investigation. The operators do not need to actively look at cameras or certain alarms. They will be notified when an alarm is activated and have instant video playback available to evaluate the condition and dispatch the appropriate response. This not only eliminates errors and omissions but also reduces the number of staff members necessary to monitor these systems because the systems have been transformed from passive to active.

The current video management system by Lenel lends itself well to being integrated with disparate systems and multiple forms of technology. As described, this allows the University to work more efficiently with less reliance on personnel while, in most cases, providing an even greater level of security by removing human error.

Based on our conversations with staff who know the system and its components we found that one drawback of the Lenel system, is the cost. Lenel products appear to be at the higher end of pricing for similar technologies. However, the University should not discontinue its efforts based on the cost of using

one product. As we stated earlier, we believe the University must engage in a process to standardize equipment and this will present an opportunity to evaluate all current hardware and software platforms against others based on the needs of the University, scalability and value.

As we mentioned during our essential challenges, the University has not developed a campus-wide acceptable usage policy. It is critical that the University develop this policy several reasons.

First, the policy will spell out the purpose and scope of camera use. This can be of great value in allaying any possible concerns of community members regarding the use of cameras. We commonly hear concerns over privacy and the use of cameras in public places similar to those we heard at Boise State. An acceptable usage policy can set both the expectations and limitations of camera use.

Second, the policy should describe the necessary training required to operate the system, as well as recording standards and standards for disseminating the video. The policy should also be in accordance with other university policies such as non-discrimination.

Finally, the policy must reassure community members that there is a quality assurance program in place that will regularly review all elements of the policy to ensure compliance.

We met with multiple students on campus to discuss Boise State's desire to expand their use of cameras. One concern they expressed was the students' right to privacy and the feeling of being "watched." The students were not aware of any existing policy and really did not understand what the cameras are used for, where they are and who, if anyone, views them. After discussing the University's plan, the value of security cameras and the authority and limitations of an acceptable usage policy, 100 percent of the students expressed support for the use of cameras.

MHA toured the campus and surrounding area on foot, by golf cart and by car during the daytime and evening to identify locations where additional cameras could add value to the current security program by augmenting staff as a force multiplier.

Based on our site survey and discussions with Campus Security officers who have previously identified campus "hot spots" and the University's desire to expand the use of security cameras on campus, we believe the University should enter into a multi-phase security camera enhancement project to install additional cameras in critical areas surrounding the campus.

The following represents locations that should be considered as part of each phase based on criticality, vulnerability and cost. These locations are also represented in the graphic illustration attached to this report.

PHASE I

- Greenbelt - Utilizing the existing infrastructure, affix fixed cameras on top of each emergency phone from the stadium parking lot to the northeast of the Morrison Center on Cesar Chavez Lane. According to the emergency phone map, these are;

  o Emergency Phone 100

  o Emergency Phone 115

  o Emergency Phone 119

  o Emergency Phone 121

  o Emergency Phone 205

  o Emergency Phone 208

  o Emergency Phone 213

- Friendship Bridge – Place cameras on the north side of the Friendship Bridge to capture the foot traffic coming on and off the bridge
- Student Union Building – Place fixed cameras around the student union and the connection paths leading to and from the building. In addition, install fixed cameras on the emergency phone at the intersection of University Drive and Lincoln Avenue to provide coverage of vehicles turning on and off University Drive.
- Brady Street Garage – Install fixed cameras at each point of entry and exit to the garage and at each pay station. In addition, install fixed cameras on the first level façade on the southwest corner to cover University Drive and vehicles heading south and southeast.
- Lincoln Avenue Garage – Install fixed, day/night cameras at each entrance and exit to the garage and at each pay station. Also, install fixed first level fixed cameras to the west façade of the garage to cover the pathway to Lincoln Rec Field. In addition, install fixed cameras on the emergency phone on the south side of University Drive at the intersection of Lincoln Avenue to provide coverage of vehicles turning on and off University Drive.

PHASE II

- Bronco Stadium – Install a combination of fixed and PTZ cameras in the west stadium lot and east stadium lot to include coverage of the intersection of Broadway and University Drive.
- Administration Visitor Lot – Install a combination of fixed and PTZ cameras in the lot to cover the points of entry, exit and parking kiosks.
- Liberal Arts Lot – Install a combination of fixed and PTZ cameras to cover entrances and stalls.

- Kinesiology Annex Path – Install fixed cameras to the Kinesiology Building to cover the east side of the tennis courts.
- Appleton Tennis Center Building – Install fixed cameras to cover the pathway directly north of the tennis courts.
- Student Recreations Center – Install fixed cameras to cover the facility entrances, and install fixed PTZ cameras on the southwest, southeast, northwest and northeast corners of the building to capture the approach from University Drive and Belmont Street.
- Albertson Library – Install fixed cameras on the façade of the south, southwest and southeast corners of the building to cover the library entrance and administrative quad pathways.

PHASE III

- Install fixed cameras to all exit and entrance points at each first year residence hall.
- Emergency Phone 440 – 1910 Boise Ave.
- Emergency Phone 500 – 860 SHRWD
- Emergency Phone 510 – 970 LUSK
- Emergency Phone 127 – 200 University Drive
- Emergency Phone 117 – 2055 Cesar Chavez Ave.
- Emergency Phone 123 – (south side of Albertson Library
- Emergency Phone 223 – 1190 University Drive
- Emergency Phone 200 – 1800 University Drive
- Emergency Phone 201 – 1607 Cesar Chavez Ave.
- Emergency Phone 400 – 2550 Boise Ave.
- Emergency Phone 410 – 1311 CHWAY
- Emergency Phone 412 – 1301 CHWAY
- Emergency Phone 413 – 1609 CHWAY
- Emergency Phone 414 – 1305 CHWAY
- Emergency Phone 228 – 1476 Bronco Circle
- Emergency Phone 355 – 1102 Lincoln
- Emergency Phone 356 – 1106 Lincoln
- Emergency Phone 354 – 1529 Belmont
- Emergency Phone 350 – 1529 Belmont

- Emergency Phone 315 – 1375 University Drive
- Emergency Phone 366 – 1295 University Drive
- Emergency Phone 226 – 1356 University Drive

Recommendations

11. Develop a campus-wide acceptable usage policy for security cameras. This policy should at least include the purpose and scope of the cameras, who has authority over them and their responsibilities, as well as the principles and procedures associated with the cameras.
12. Develop security camera equipment design standards that detail the minimum requirements, i.e. whether the cameras should be analog, IP, day/night/ color, megapixel, fixed, PTZ, etc., as well as mandatory camera locations and minimum recording rates.
13. Develop video management system requirements that include: retention periods, data security protocols, video retrieval, distribution and chain of custody.
14. Install additional security cameras based on the phased roll-out described earlier in this section of the assessment.

ALARMS

Contemporary Standard

There are three basic and common types of alarms utilized for security purposes at college and universities. These are: burglar alarms, duress or "panic" alarms and typically, door held/forced open alarms integrated into an electronic access control system.

Burglar alarms or "intrusion" alarms can have a number of peripheral devices or hardware associated with them, such as glass break detection, motion detection and passive infrared sensors, and they can be wired or can even be wireless. The typical intrusion alarm monitors points of entry such as doorways, glass windows, roof access and interior spaces such as large classrooms or hallways.

Duress or "panic" alarms come in a variety of forms but are typically surface mounted "buttons" that allow an individual to send a remote signal to security, police or a central monitoring station in the case of an emergency. It is common to see the devices in areas such as nearby cash registers, counseling centers, mail centers, recreation centers and executive or senior leadership office areas.

Finally, as electronic access control systems have become more of a standard at colleges and universities, we see an increase in the use of door forced, held or propped open alarms. As with burglar alarms, these alarms indicate

a change in door status and send a signal that notifies an operator through the access control system.

In each case, these alarms are used to alert someone about a potential problem within a university facility. There is no empirical data to suggest how colleges and universities usually monitor these alarms (in house vs. central station) and we believe each situation is unique and should be evaluated based on the number of alarms on campus, available resources and cost analysis.

The decision to install any alarm should be based on risk and criticality. For that reason, many college and universities require each unit at the institution to be in contact with a single source, such as police, public safety or security staff to determine if the installation of an alarm is reasonable and required for the particular application.

Observations

Boise State University uses a combination of alarms as described in the contemporary standard. A number of alarms are monitored by the Campus Security Department while some are farmed out to Mountain Alarm.

As with other areas of security technology, the University does not have an acceptable usage or policy statement regarding the use of intrusion or duress alarms on campus. This is a recurring theme and one that we will continue to encourage the University to address.

Our first observation is that the University utilizes a central station to monitor certain alarms on campus. Like other forms of technology, this practice may have grown over the years because of a lack of ownership. However, we believe all alarms can and should be monitored at Campus Security Headquarters.

There are several reasons for this. First, the report of alarms that dial to an outside central monitoring station will typically be delayed due to relays, phone calls and verification. Second, because individual departments can order and pay for their own alarm systems without the approval of a centralized department or contact, many alarms are monitored under various service contracts and at different costs per month. So not only is the University failing to appropriately leverage its buying power and vendor relationships, it may not need to pay for the service at all.

Based on our observations and discussion, we believe the Boise State Campus Security Department is fully capable of monitoring, dispatching and responding to intrusion and duress alarms on campus. This can be accomplished by routing the signal to the Dispatch Center rather than a central station, as is the procedure now for some alarms. While we were unable to identify how many individual alarm contracts exist, we do know alarm monitoring can range in value from $20 - $30 per month. If we assume the University has 100 alarm accounts at an average cost of $25 per month, we could estimate the University may be currently paying approximately $30,000

per year for alarm monitoring. We believe the Campus Security Department could monitor the same alarms for substantially less fees.

For example, Campus Security might need to purchase additional software, and conduct operator training to completely assume this role. Based on a number of variables including alarm monitoring software and training options, it is possible that in year 1, the same $30,000 in savings would be reallocated to accomplish these tasks. However, assuming Campus Security receives adequate training, monitoring software, and maintenance agreements, the same departments could be charged a much lower rate and the fees would be moved to the Campus Security Department to sustain the costs of providing the monitoring. And while there would still be a cost individual departments, the cost savings could be as much as 50 percent and the overall sum would be budget neutral for the University since the monies would stay within the University.

While we discussed this idea with some members of the Dispatch staff, there was some concern that the increased volume of alarms could overwhelm Campus Security dispatchers. Based on what we observed and heard, we did not see any evidence to suggest that the task of monitoring all campus alarms would be onerous or extraordinarily burdensome on the Dispatch staff.

Secondly, the University does not have a campus-wide facility standard for the use of alarms nor does it engage in a risk-based, approach to the installation of alarms. That's not to say that care is not taken during the planning phase of construction, however the large number of existing systems appear to have been installed by individual departments at their discretion.

The Department of Campus Security does have a strong position on the use of duress or panic alarms. However, while we visited campus, we learned of multiple facilities and departments requesting these devices to be installed. In many cases, these requests were based on a perceived need to alert others of a potential problem. In others, it seemed to be based on the fact that someone else had one installed in their office and it seemed therefore seemed appropriate to request one for themselves.

The decision to install any type of alarm should be based on a number of factors including the type of asset being protected, known or likely threats, vulnerability, criticality, geography, historical acts, effectiveness and cost.

We believe the University would benefit from a risk-based, decision-making matrix as part of a comprehensive alarm policy to determine the appropriate installation and use of alarms.

We also believe the University should continue to expand its use of door prop, forced and held open alarms through the access control system. While these alarms can at times be considered nuisance alarms due to the large number of false alarms that can be inadvertently activated, they can also alert security forces of changes in door status and prompt an immediate response.

We believe these alarms are significantly valuable in not only residential facilities, but critical areas of campus, as noted in the Department of Homeland Security's Site Assistance Visit (SAV), report to Boise StateDe. Door contacts and relays are inexpensive, durable and reliable.

In addition, the use of alarm monitoring software can be integrated to include campus security camera systems and door alarms as noted in our review of security cameras. This is an additional feature that creates efficiencies by eliminating the need for active camera monitoring and human error.

Recommendations

15. Develop an alarm installation and monitoring policy.
16. Consider requiring all intrusion alarms to report directly to Campus Security
17. Consider reallocating alarm fees currently paid to third party vendors to Campus Security to maintain and support alarm-monitoring activities.
18. Develop facility and equipment standards for the use of intrusion detection systems.
19. Develop a risk-based decision matrix to determine where alarms should be installed and what type of alarms should be approved for installation
20. Continue to expand the use of door prop, forced and held open alarms in all residential and high-risk facilities

SECTION V – MASTER LIST OF RECOMMENDATIONS AND MATRIX

1. Create a new position responsible for security systems and technology including, but not be limited to, the development of security technology standards, design standards, oversight of security systems, systems integration and physical security surveys and assessments. This individual would report to the Security Technology Working Group.
2. Establish campus-wide security standards. Campus-wide security standards are a promising practice that institutions are implementing as they commit considerable resources to security technology. The overall goal of such a standard is to ensure that buildings are "security-smart" given reasonably foreseeable threats and available resources. These standards should include building-specific security technology system designations that specify the types of security systems that the University would expect for specific types of buildings.
3. Assign the Department of Campus Security as the formal operational or "business" owner of security technology and security systems.
4. Create a Security Technology Working Group. Accordingly, the new position referenced in recommendation #1 should chair this committee.
5. Develop campus-wide security technology system equipment standards. Determine common equipment hardware, manufacturers, models, capacities and software that are easily integrated with other systems at the University.
6. Select a nationally recognized value added reseller (VAR) with the capacity to meet the needs of the University to purchase and install University-approved security systems while leveraging centralization to reduce overall costs.
7. Develop comprehensive policies related to each specific security technology. These policies should not only cover the purpose, scope and acceptable use of each technology but also the procurement process.
8. Engage in a campus wide assessment to identify and inventory all security systems currently being utilized throughout the University. These should at least include security cameras, intrusion alarms, duress alarms, and electronic access control readers.
9. Wherever possible, make an effort to integrate disparate, legacy security systems into one common platform that includes all devices and security system countermeasures that terminate at the Campus Security building. Under the current system, individual departments that have previously installed security systems replace or upgrade these systems on an as-needed basis. However, we can only assume that service, maintenance,

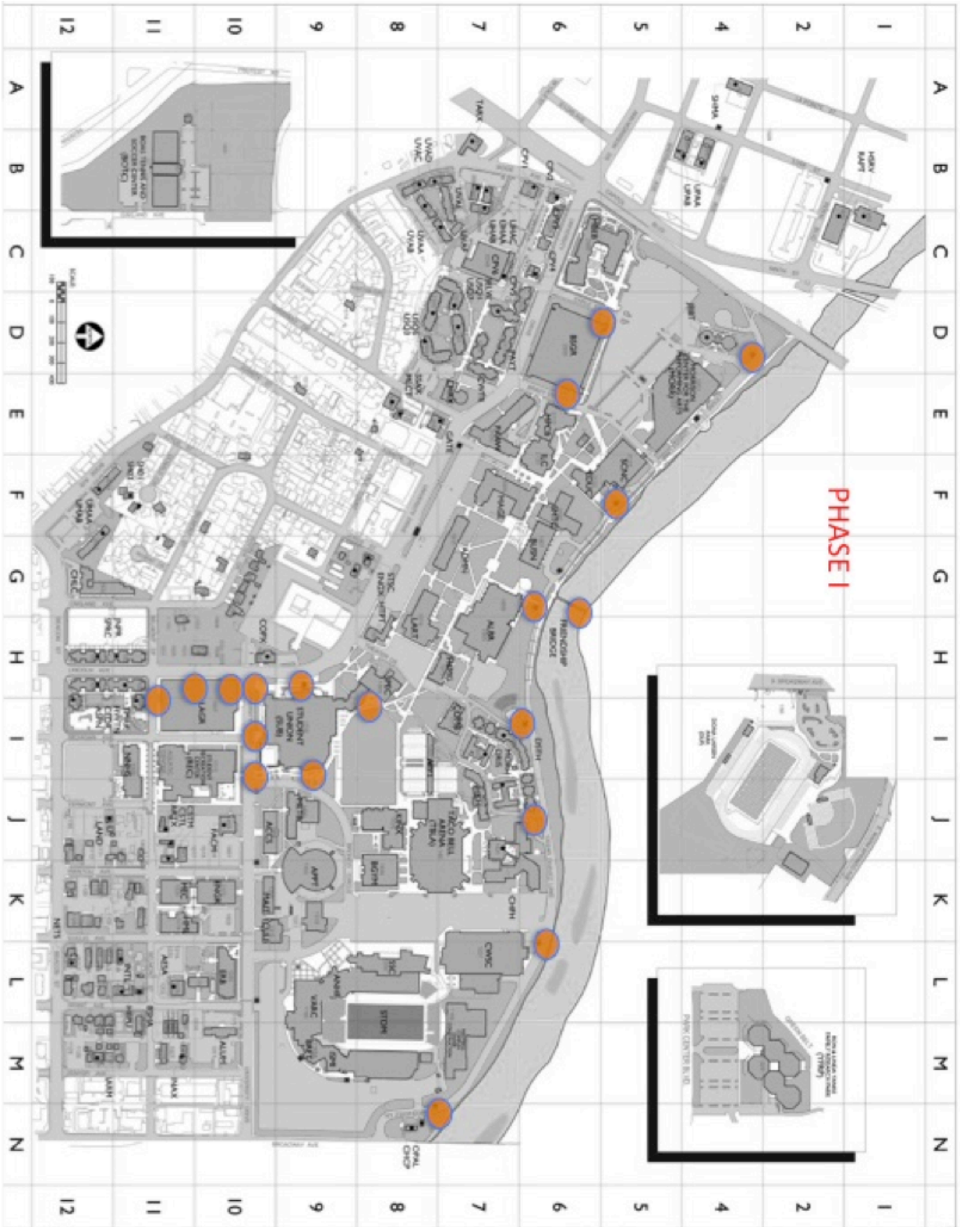
and upgrades must be completed because the university is not aware of all the systems currently in place. Integrating the systems will maximize the University's return on investment.

10. As the University embarks on the development of University-wide security standards and facility design standards, we suggest an initiative to ensure that all existing building security systems comply with the new standards. Clearly, this is a process that must be phased in over a period of years based on available time and resources.
11. Develop a campus-wide acceptable usage policy for security cameras. This policy should at least include the purpose and scope of the cameras, who has authority over them and their responsibilities, as well as the principles and procedures associated with the cameras.
12. Develop security camera equipment design standards that detail the minimum requirements, i.e. whether the cameras should be analog, IP, day/night/ color, megapixel, fixed, PTZ, etc., as well as mandatory camera locations, and minimum recording rates.
13. Develop video management system requirements that include retention periods, data security protocols, video retrieval, distribution and chain of custody.
14. Install additional security cameras based on the phased roll-out described earlier in this section of the assessment.
15. Develop an alarm installation and monitoring policy.
16. Consider requiring all intrusion alarms to report directly to Campus Security.
17. Consider reallocating alarm fees currently paid to third party vendors to Campus Security to maintain and support alarm-monitoring activities.
18. Develop facility and equipment standards for the use of intrusion detection systems.
19. Develop a risk-based decision matrix to determine where alarms should be installed and what type of alarms should be approved for installation.
20. Continue to expand the use of door prop, forced and held open alarms in all residential and high-risk facilities.

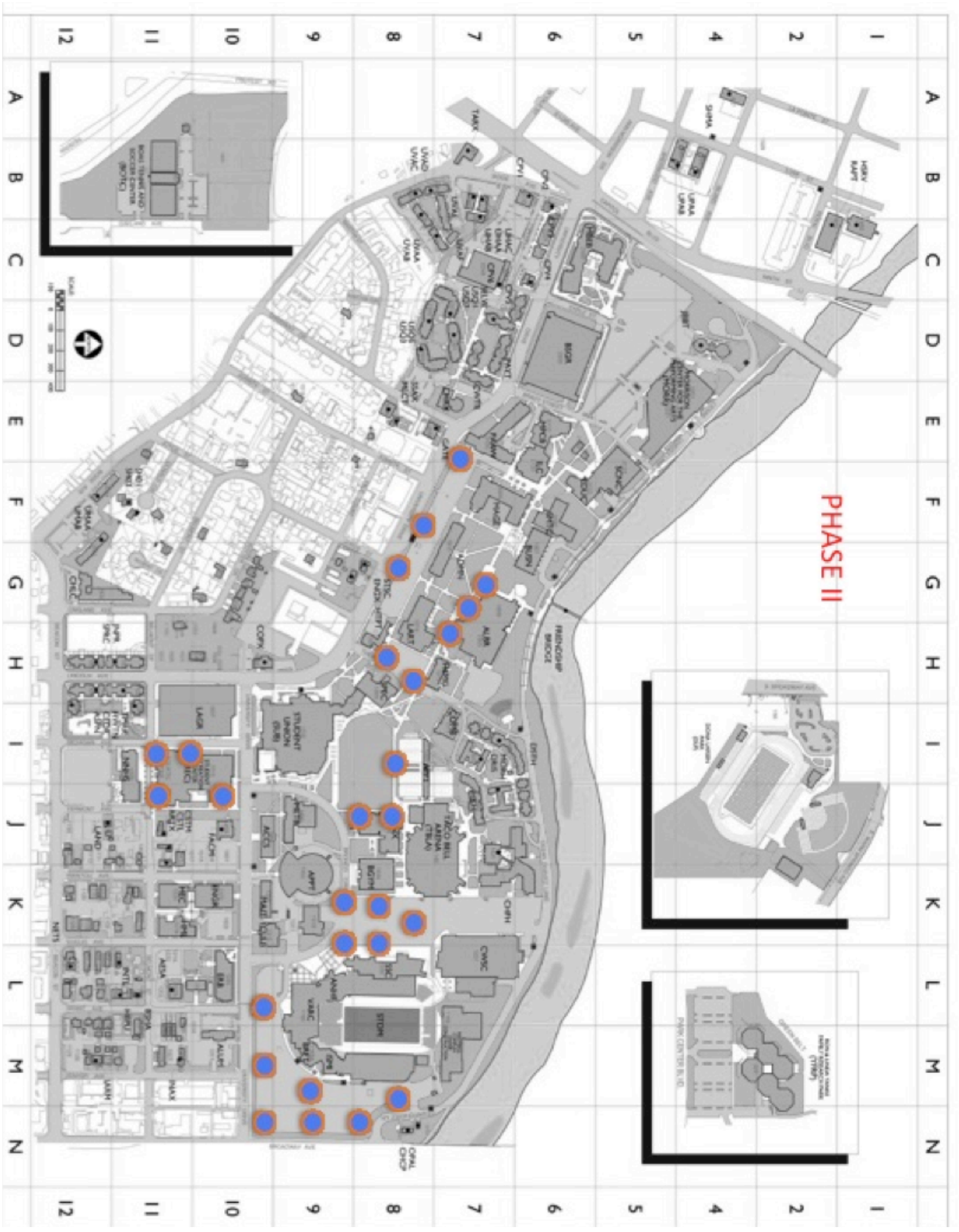
RECOMMENDATION MATRIX

RECOMMENDATIONS MATRIX	FY 14 COST LOW	FY 14 COST MEDIUM	FY 14 COST HIGH	FY 14 CRITICALITY LOW	FY 14 CRITICALITY MEDIUM	FY 14 CRITICALITY HIGH	FY 15 COST LOW	FY 15 COST MEDIUM	FY 15 COST HIGH	FY 15 CRITICALITY LOW	FY 15 CRITICALITY MEDIUM	FY 15 CRITICALITY HIGH	FY 16 COST LOW	FY 16 COST MEDIUM	FY 16 COST HIGH	FY 16 CRITICALITY LOW	FY 16 CRITICALITY MEDIUM	FY 16 CRITICALITY HIGH
PHYSICAL SECURITY APPROACH																		
1. Create a new position responsible for security systems and technology.			x		x													
2. Establish campus-wide security standards for different facility types.	x				x													
3. Assign Campus Security as the business owner for secuity technology.	x					x												
4. Create a Security Technology Working Group.	x				x													
5. Develop campus-wide security system equipment standards.	x				x													
6. Select a Value Added Reseller and Integrator to install University approved systems while leveraging centralization to reduce overall costs.	x					x												
7. Develop University policy related to each specific technology.	x				x													
8. Engage in a campus-wide assessment to inventory all security systems utilized throughout the University campus.		x				x												
9. Where possible, integrate disparate, legacy security systems to one common platform.								x			x							
10. Begin a phased project to bring all buildings up to newly developed standards.														x			x	
SECURITY CAMERAS																		
11. Develop a campus-wide acceptable usage policy for security cameras.	x					x												
12. Develop security camera equipment design standards that detail minimum requirements.	x				x													
13. Develop video management system requirements that include retention periods, data security protocols, video retrieval, distribution and chain of custody.		x				x												
14. Install additional security cameras based on 3 year, phased approach.																		
Phase I			x		x													
Phase II									x		x							
Phase III															x		x	
ALARMS																		
15. Develop alarm installation and monitoring policy (for all types of alarms).	x				x													
16. Consider requiring all intrusion alarms to report to Campus Security.								x		x								
17. Consider reallocating alarm fees currently paid to third party vendors to Campus Security to maintain and support alarm-monitoring activities							x			x								
18. Develop facility and equipment standards for the use of intrusion detection.	x				x													
19. Develop a risk-based decision matrix to determine where alarms should be installed and what type of alarm should be approved.							x				x							
20. Expand the use of door pro, forced and held open alarms in all residential and high-risk facilities.														x			x	

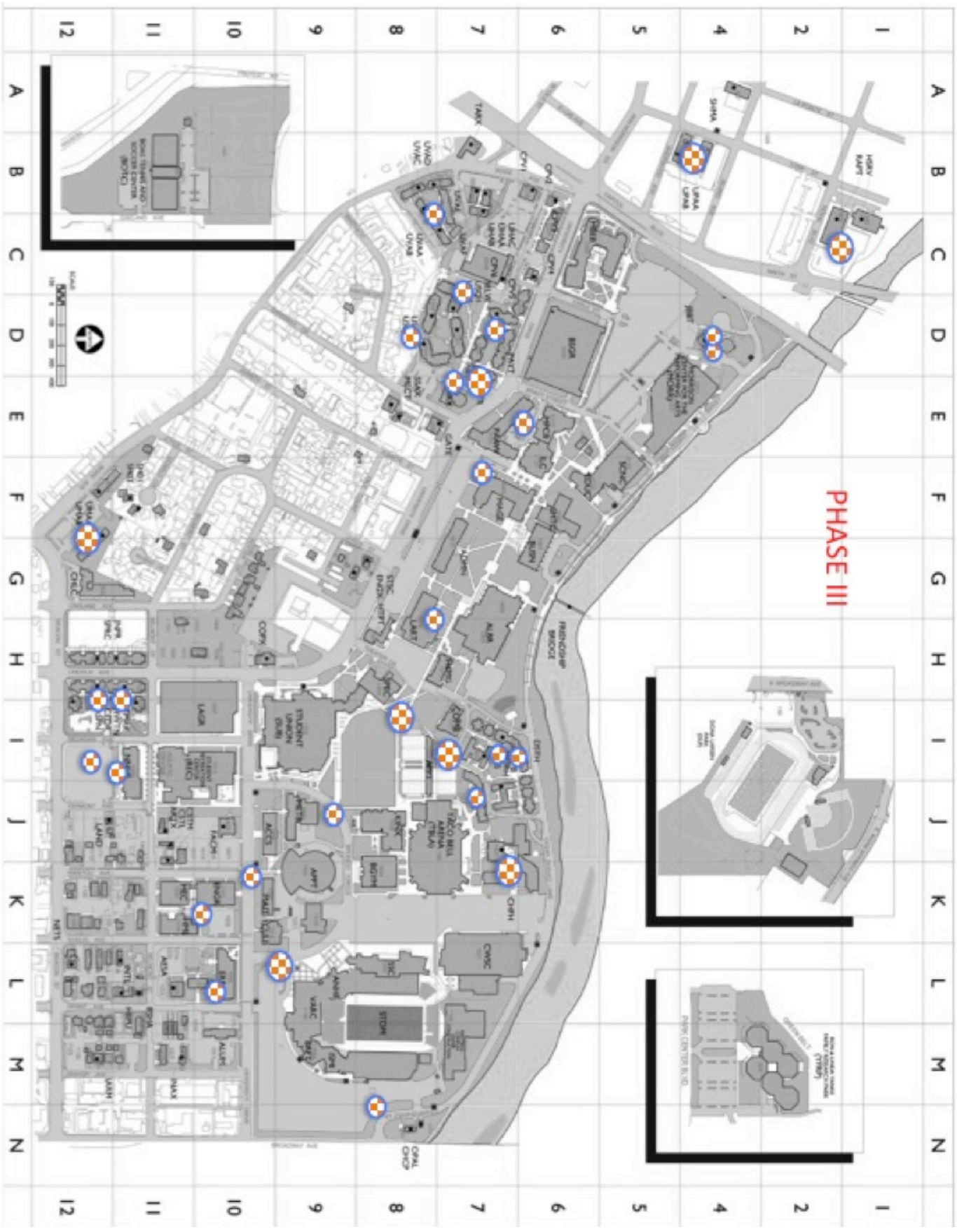
PHASE I – CAMERA INSTALLATIONS



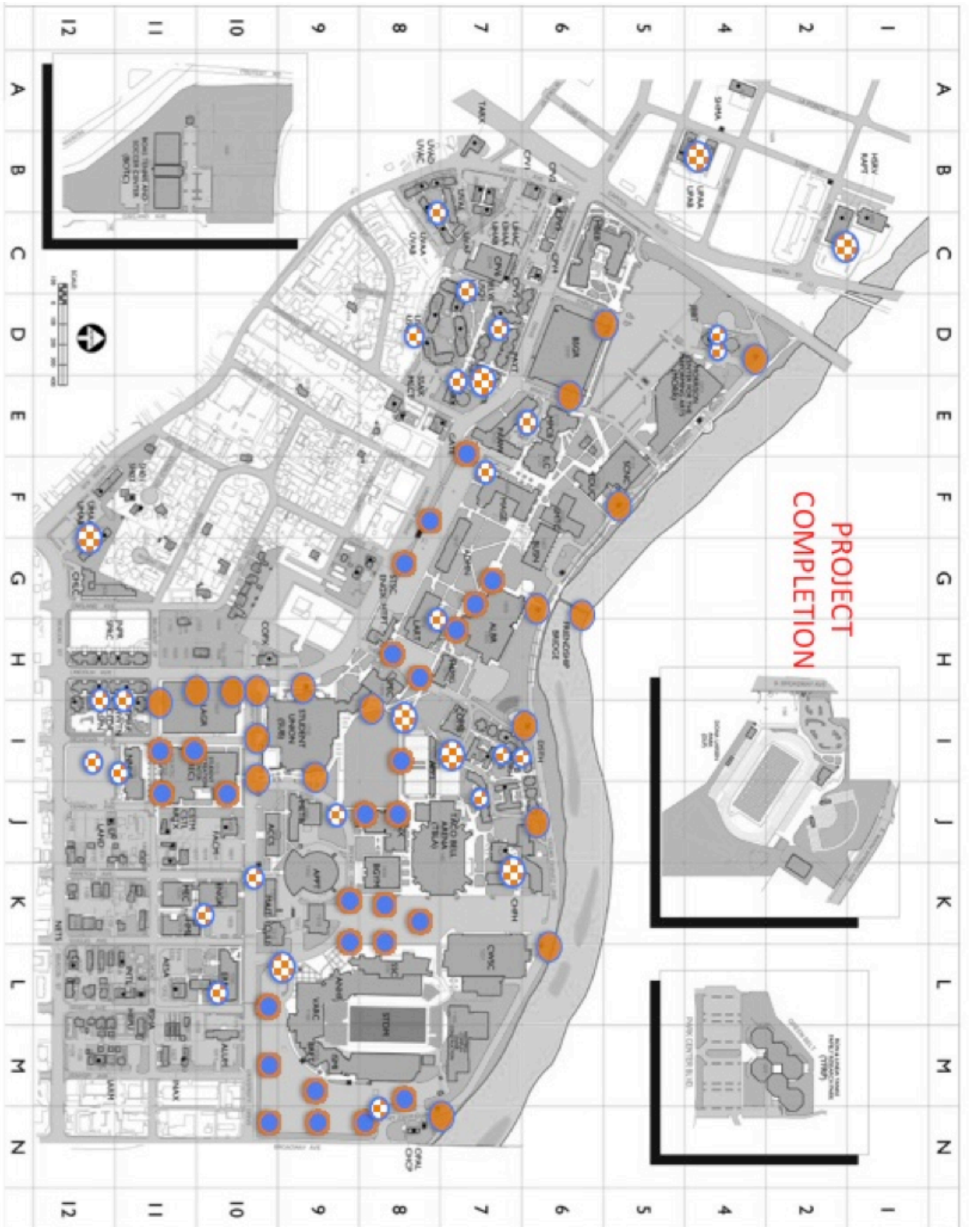
PHASE II – CAMERA INSTALLATIONS



PHASE III – CAMERA INSTALLATIONS



ALL PHASES COMPLETED - OVERVIEW



SECTION VI – FIRM DESCRIPTION AND QUALIFICATIONS

Margolis Healy & Associates, LLC, is a professional services firm specializing in higher education safety and security. Our focus includes, but is not limited to, campus facility security assessments: emergency operations response training and policy development; behavioral threat assessment team development and case-by-case threat assessment consultation; campus public safety management studies and assessment centers; litigation consultation; security technology audits; *Clery Act* documentation audits; and campus public safety arming studies & deployment strategy development. In January 2008, after more than fifteen years each of providing consulting services to clients in the education, public and private sectors, Dr. Gary J. Margolis and Mr. Steven J. Healy merged their practices, Margolis & Associates, LLC and Strategic Security Consulting, LLC, into Margolis Healy & Associates, LLC. Their combined experience has quickly catapulted MHA into one of the leading professional services firms for safety and security needs at universities, colleges and K-12 school systems.

Our team of professionals brings a diverse set of skills and expertise to client institutions ranging from large public universities to private institutions, community colleges and K-12 school districts.

Mr. Healy and Dr. Margolis have been intimately involved in the national discussion on mass notification for college campuses, including Mr. Healy's testimony before the United States Congress. They have relationships with the industry's leading providers and have published articles and participated in related webinars on the topic. The MHA emergency notification principles of "Timely, Accurate, and Useful (TAU)" and "Alert, Inform, Reassure (AIR)" have become industry taglines and found their way into testimony and legislation. Our mass and emergency notification template messages, available free through our website, are being used by universities and colleges across the country.

Dr. Margolis, Mr. Healy and their team have personally managed or been intimately involved with scores of critical incidents on college campuses ranging from violent crime to natural disasters (including the 9/11 tragedy and its impact on the schools in NYC). We have first-hand experience in crisis response and recovery planning and operations at institutions of higher education. In 2008, Dr. Margolis was contracted to review the next iteration of FEMA's emergency action guides for educational settings.

Mr. Healy and Dr. Margolis are the lead authors of the International Association of Campus Law Enforcement Administrator's *Blueprint for Safer Campuses: An Overview of the Virginia Tech Tragedy and Implications for Campus Safety*. This document, unveiled at a press conference sponsored by the Woodrow Wilson School at Princeton University on April 18, 2008, is a roadmap for campus safety and security. In 2006, Mr. Healy was selected to serve as a faculty

member for the first-ever comprehensive, collaborative Clery Act training sessions funded by a U.S. Department of Justice grant. As a certified instructor for this program, he has provided training at several programs delivered across the country.

Shortly after the Virginia Tech incident, the President of The National Association of Attorneys General (NAAG), Georgia Attorney General Thurbert Baker, determined to establish an ad hoc Task Force on School and Campus Safety (Task Force) to consider what had transpired since the issuance of the previous NAAG report in 1999, including the incident at Virginia Tech, and issue a report making updated recommendations regarding the prevention of, and response to, violence in schools and on college campuses. Mr. Healy participated in the development of this report, *The National Association of Attorneys General Task Force on School and Campus Safety.*

In 2008, Dr. Margolis was contracted to review the next iteration of the Federal Emergency Management Department's *Incident Action Guides* to assure their relevancy to the higher education environment.

Margolis Healy & Associates was recently awarded a U.S. Department of Justice, Community Oriented Policing Services (COPS) Office competitive grant to develop and deliver a behavioral threat assessment curriculum for universities and colleges across the nation (www.CampusThreatAssessment.org). We help institutions of higher education develop and implement a threat assessment capacity that fits within their unique cultures and that is effective in both preventing violence and helping persons in need. We train higher education institutions on how to create and implement a threat assessment team (or add threat assessment capabilities to an existing team) and how to identify, investigate, evaluate, and intervene with persons and situations that raise concern on campus. We also consult on individual threat cases and provide guidance on crafting or revising institutional policies and procedures to facilitate effective threat assessment and collaborative case management.

The MHA Methodology

Margolis Healy & Associates serves our clients through the development of a Risk Tolerance Profile that assists the institution with identifying the range of realistic threats and vulnerabilities it faces, and then implementing a decision making process to determine which require prevention, mitigation and/or response plans. Without such a process, universities and colleges face the daunting task of giving equal attention to all perceived and real threats. Our process recognizes the range between high impact/low probability and low impact/high probability events. The active shooter tragedy (high impact/low probability) and the iPod theft from the library (low impact/high probability) each require different strategies. Impact is defined through the institution and the individual.

MHA has developed a unique, proprietary methodology for evaluating safety and security needs at institutions of higher education based on years of educational campus safety and security experience, research, reflection and evaluation. We assess safety and security at educational institutions through our proprietary 3 Circles of Prevention System.™ We have extensive proprietary checklists that support our methodology.

The First Circle asks to what extent relationships and services exist for early interception and intervention for problems and issues germane to faculty, staff and students. Such services may include drug and alcohol education and counseling, behavioral threat assessment teams, grievance policies, workplace violence policies and prevention systems, sexual assault, stalking and domestic violence victim advocacy; mediation services and grievance policies and procedures for faculty and staff; and other similar policies and services that address problems before they become a crisis.

The Second Circle explores the extent to which institutions of higher education have employed physical obstacles, delaying tactics and security technology to control, secure or regulate access to the physical plant. This may include systems that direct vehicular traffic; security cameras; networked or standalone door locking systems and hardware; campus lighting (interior and exterior); E911 capacity and PBX phone systems; mass notification systems (high and low technology); fire and life safety systems; visitor management policies and practices; inclusion of crime prevention through environmental design considerations; and access control and other security technology tools.

The Third Circle explores measures that enable the institution to respond to events and security and safety related needs in an organized, timely, and efficient manner. This may include a public safety function with organized involvement of students, faculty and staff in the security of the campus; memoranda of understanding with area police, fire and emergency medical services; emergency response and recovery systems, policies and procedures that have been trained to; and adoption and implementation of the National Incident Management System (NIMS) and the Incident Command System (ICS). Combined, this third circle of prevention builds capacity for the human response to safety and security requirements.

Taken together, the various strategies depict the interconnected nature of campus safety and security. Changes or decisions made to one area impact the others. The deployment of security technology (cameras, door prop alarms, controlled access points) may or may not have an effect on the number of public safety officers, which may or may not impact other security needs. MHA works with our clients to develop a reasonable campus safety and security program based on their current state and the desired future state.

The measures taken to address safety and security are as much data and metrics driven as they are based on perception. We believe that our expertise,

knowledge and experiences uniquely qualify us to assist our client institutions with recommendations tuned to their culture and needs.

Margolis Healy & Associates, LLC is a minority and veteran-owned small business. For a complete listing of available services, please visit www.margolishealy.com.

Margolis, Healy & Associates, LLC
445 Greystone Drive
Richmond, Vermont 05477-7700
866.817.5817 (toll free & fax)
Email: info@margolishealy.com

www.CampusSentinel.com

www.margolishealy.com